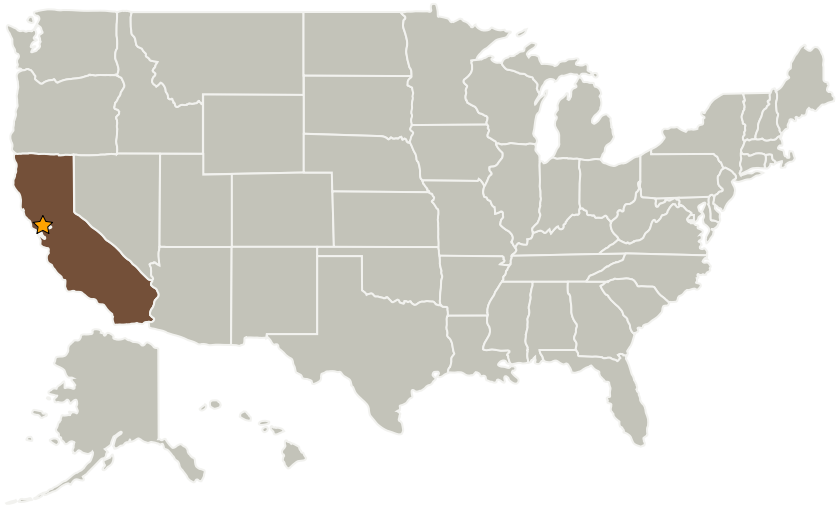
Failsafe, Phase II

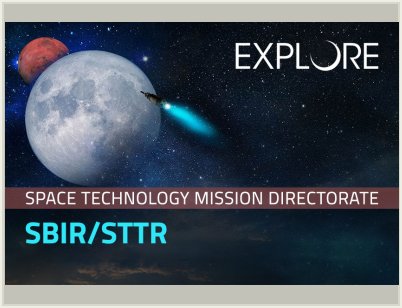
Completed Technology Project (2007 - 2009)

Project Introduction

With embedded software becoming ever more complex, assuming that it behaves perfectly is not realistic. The adaptation of fault protection concepts to embedded software is attractive, particularly in the context of the fault containment and health management capabilities provided by ARINC 653. In Phase II we shall develop tools to define simple, verifiable models that characterize the software with respect to its interface behavior, resource usage, and data reasonableness. We shall provide a software framework to instrument and monitor the software as it executes in both test and operational environments. When a deviation from the model is detected, a simple remediation action, including a hard or soft component reset is invoked. These tools will be integrated into ARINC 653 to support fault detection and recovery in an operational context, and the Eclipse software development environment for application in a test and verification context such as DSIL and engineering analysis context such as CEAL. Further we shall produce a methodology to assist in certification of instantiations of our software fault protection framework.

Primary U.S. Work Locations and Key Partners





Failsafe, Phase II

Table of Contents

Organizational Responsibility

Responsible Mission Directorate:

Space Technology Mission Directorate (STMD)

Lead Center / Facility:

Ames Research Center (ARC)

Responsible Program:

Small Business Innovation Research/Small Business Tech Transfer

Failsafe, Phase II

Completed Technology Project (2007 - 2009)

Organizations Performing Work	Role	Type	Location
★Ames Research Center(ARC)	Lead Organization	NASA Center	Moffett Field, California
Kestrel Technology LLC	Supporting Organization	Industry	Palo Alto, California

Primary U.S. Work Locations
California

Project Management

Program Director:

Jason L Kessler

Program Manager:

Carlos Torrez

Technology Areas

Primary:

- TX11 Software, Modeling, Simulation, and Information Processing
  - TX11.1 Software Development, Engineering, and Integrity
    - TX11.1.4 Operational Assurance